AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials, the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a desktop computer, wherein the authentication request includes a first set of credentials of the user, the first set of credentials comprising a username and a password;

determining based on the first set of credentials being a username and password that a first credential store is to be accessed to validate the authentication request from the desktop computer, the first credential store storing sets of credentials that each comprise a username and password;

validating the first set of credentials provided by the user by accessing the first credential store to determine whether the username and password are associated with a single unique user identifier, wherein ~~the first~~each set of credentials in the first credential store ~~are~~ is associated with a single unique user identifier of ~~the~~ a user, a single unique user account, and a single unique user profile such that upon determining that the first set of credentials is associated with a unique user identifier, the unique user identifier is returned to the desktop computer such that the desktop computer may use the unique user identifier to access a service;

receiving a second authentication request at the authentication system from a cellular phone, wherein the authentication request includes a second set of credentials of the user, the second set of credentials comprising a numeric username and a numeric pin, wherein the numeric username is distinct from the username;

determining based on the second set of credentials being a numeric username and a numeric pin that a second credential store is to be accessed to validate the authentication request from the cellular phone, the second credential store storing sets of credentials that

each comprise a numeric username and a numeric pin; and

validating the second set of credentials provided by the user by accessing the second credential store to determine whether the numeric username and numeric pin are associated with a single unique user identifier, wherein ~~the second~~each set of credentials in the second credential store ~~are~~ is also associated with ~~the~~ a single unique user identifier of ~~the~~ a user, ~~the~~ a single unique user account, and ~~the~~ a single unique user profile such that upon determining that the second set of credentials is associated with the same unique user identifier as the first set of credentials, the unique user identifier is returned to the cellular phone such that the cellular phone may use the unique user identifier to access the service.~~, such that the user may access the single unique user account by entering either the first set or the second set of credentials.~~

2-3. (Canceled)

4. (Currently Amended) The method as defined in claim 46, wherein the act of receiving a new set of credentials from the user further comprises storing the new set of credentials in a third credential store based on a type of the new set of credentials~~an act of symmetrically associating the new set of credentials with a unique user identifier~~.

5. (Canceled)

6. (Currently Amended) The method as defined in claim 4, wherein ~~the act of symmetrically associating the new set of credentials with a unique user identifier~~ storing the new set of credentials further comprises an act of caching a copy of the unique user identifier with the new set of credentials.

7. (Currently Amended) The method as defined in claim 1, wherein the ~~act of receiving the new~~first set of credentials is a primary set of credentials,~~from the user further comprises an act of asymmetrically~~ the method further comprising associating the ~~new~~ second set of credentials with ~~a primary~~the first set of credentials~~, wherein the primary set of credentials~~

~~is stored in a primary store with the unique user identifier~~.

8. (Previously Presented) The method as defined in claim 46, further comprising one or more of:

a step for remembering which set of credentials was received in the authentication request;

a step for prompting the user for a more secure set of credentials when the set of credentials received in the authentication request do not meet security requirements of the service, such that the user selects a new set of credentials from among the plurality of sets of credentials valid at the authentication system; and

a step for providing at least one security measure for each set of credentials associated with the user account, wherein the user is not authenticated to a service if the security measure of a particular set of credentials is breached or the user account is locked.

9. (Currently Amended) The method as defined in claim 1, wherein the unique user account corresponds to the~~a~~ service, the method further comprising:

receiving an authentication response from the authentication system, wherein the authentication response includes the unique user identifier that authenticates the user to the service, the response also including the user profile; and

sending an authenticated request to the service, wherein the authenticated request includes the unique user identifier and user profile such that access to the service is obtained.

10-21. (Canceled)

22. (Previously Presented) The method as recited in claim 46, wherein the new set of credentials has an associated security level and wherein the user has attempted to authenticate using the first set of credentials and wherein the method further comprises:

associating the new set of credentials with the user account such that the user can be authenticated with any of the plurality of sets of credentials,

prior to providing the response, and subsequent to receiving the authorization

request, prompting the user for a secure set of credentials that is more secure than the first set of credentials if the security level of the first set of credentials is insufficient for a service being accessed by the user, wherein the service is provided with the security level of both the first set of credentials and the secure set of credentials, but is not aware of either the first set of credentials or the secure set of credentials.

23. (Previously Presented) The method as defined in claim 22, wherein the step for associating the new set of credentials with the user account further comprises a step for symmetrically associating the first set of credentials and the new set of credentials with the user account, wherein the user account is cached with each of the first set of credentials and the set of credentials.

24. (Previously Presented) The method as defined in claim 23, wherein the step for associating the new set of credentials with the user account further comprises a step for asymmetrically associating the new set of credentials with a primary set of credentials, wherein the primary set of credentials is associated with the user account and wherein the primary set of credentials is cached with each new set of credentials.

25. (Previously Presented) The method as defined in claim 22, further comprising a step for automatically authenticating the user at different services after the user has been authenticated at a first service.

26. (Canceled)

27. (Currently Amended) In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a computer program product for implementing a method for associating multiple credentials with a user account such that the user may be authenticated with anyone of the multiple credentials, the computer program product comprising:

a computer readable storage medium storing computer readable instructions for performing a method comprising:

receiving an authentication request at the authentication system from a desktop computer, wherein the authentication request includes a first set of credentials of the user, the first set of credentials comprising a username and a password;

determining based on the first set of credentials being a username and password that a first credential store is to be accessed to validate the authentication request from the desktop computer, the first credential store storing sets of credentials that each comprise a username and password;

validating the first set of credentials provided by the user by accessing the first credential store to determine whether the username and password are associated with a single unique user identifier, wherein ~~the first~~each set of credentials in the first credential store~~are~~ is associated with a single unique user identifier of ~~the~~ a user, a single unique user account, and a single unique user profile such that upon determining that the first set of credentials is associated with a unique user identifier, the unique user identifier is returned to the desktop computer such that the desktop computer may use the unique user identifier to access a service;

receiving a second authentication request at the authentication system from a cellular phone, wherein the authentication request includes a second set of credentials of the user, the second set of credentials comprising a numeric username and a numeric pin, wherein the numeric username is distinct from the username;

determining based on the second set of credentials being a numeric username and a numeric pin that the second credential store is to be accessed to

validate the authentication request from the cellular phone, the second credential store storing sets of credentials that each comprise a numeric username and a numeric pin; and

validating the second set of credentials provided by the user by accessing a second credential store to determine whether the numeric username and numeric pin are associated with a single unique user identifier, wherein ~~the second~~each set of credentials in the second credential store ~~are~~is also associated with ~~the~~ a single unique user identifier of ~~the~~ a user, ~~the~~ a single unique user account, and ~~the~~ a single unique user profile such that upon determining that the second set of credentials is associated with the same unique user identifier as the first set of credentials, the unique user identifier is returned to the cellular phone such that the cellular phone may use the unique user identifier to access the service.~~, such that the user may access the single unique user account by entering either the first set or the second set of credentials.~~

28-29. (Canceled)

30. (Currently Amended) The computer readable storage medium of claim 47, wherein the act of receiving a new set of credentials from the user further comprises storing the new set of credentials in a third credential store based on a type of the new set of credentials~~an act of symmetrically associating the new set of credentials with the unique user identifier~~.

31. (Canceled)

32. (Currently Amended) The computer readable storage medium of claim 30, wherein ~~the act of symmetrically associating the new set of credentials with the unique user identifier~~ storing the new set of credentials further comprises an act of caching a copy of the unique user identifier with the new set of credentials.

33. (Currently Amended) The computer readable storage medium of claim 27, wherein the ~~act of receiving the new~~ first set of credentials is a primary set of credentials~~, from~~

~~the user further comprises an act of asymmetrically~~ the method further comprising associating the ~~new~~second set of credentials with the first~~a primary~~ set of credentials~~, wherein the primary set of credentials is stored in a primary store with the unique user identifier~~.

34. (Previously Presented) The computer readable storage medium of claim 27, wherein the computer readable instructions further comprise instructions for performing the acts of:

remembering which set of credentials was received in the authentication request; and

prompting the user for a more secure set of credentials when the set of credentials received in the authentication request is not sufficient for the service.

35. (Previously Presented) The computer readable storage medium of claim 27, wherein the unique user account corresponds to a service, and wherein the computer readable instructions further comprise instructions for performing the acts of:

receiving an authentication response from the authentication system, wherein the authentication response includes the unique user identifier that authenticates the user to the service, the response also including the user profile; and

sending an authenticated request to the service, wherein the authenticated request includes the unique user identifier and user profile such that access to the service is obtained.

36-40. (Canceled)

41. (Previously Presented) The method as defined in claim 1, wherein the same unique user identifier is provided to the user regardless of the set of credentials received from the user.

42. (Canceled)

43. (Previously Presented) The method as defined in claim 46, wherein providing the unique user identifier and the user profile to the device comprises sending a cookie containing

the unique user identifier and the user profile to the device.

44. (Previously Presented) The method as defined in claim 1, wherein the user profile includes data about the user comprising name, personal information, preferred language, preferences, and location.

45. (Previously Presented) The method as defined in claim 46, wherein the act of validating the first and second sets of credentials provided by the user further comprises an act of the authentication system comparing the first and second sets of credentials selected by the user against the plurality of sets of credentials stored in the credential store to determine validity.

46. (Currently Amended) The method as defined in claim 1 wherein the user selects which set of credentials to provide from among a plurality of sets of credentials valid at the authentication system and associated with the user, the set of credentials being chosen by the user based at least partially on the user's device, the method further comprising:

receiving a new set of credentials from the user~~, wherein~~ and associating the new set of credentials ~~is associated~~ with the ~~same~~ unique user identifier ~~of the user~~, the user account, and the user profile of the user;

storing the new set of credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of the multiple sets of credentials associated with the user account; and

providing, in response to the request, the unique user identifier ~~and the user profile to the device~~.

47. (Currently Amended) The computer readable storage medium of claim 27, wherein the user selects which set of credentials to provide from among a plurality of sets of credentials valid at the authentication system and associated with the user, the set of credentials being chosen by the user based at least partially on the user's device, wherein the computer readable instructions further comprise instructions for performing the acts of:

receiving a new set of credentials from the user and associating, ~~wherein~~ the new set of credentials ~~is associated~~ with the ~~same~~ unique user identifier ~~of the user~~, the user account, and

the user profile of the user;

storing the new set of credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of the multiple sets of credentials associated with the user account; and

providing, in response to the request, the unique user identifier ~~and the user profile to the device~~.

48. (Currently Amended) In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials, the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a first computer, wherein the authentication request includes a first set of credentials of the user;

determining based on a format of the first set of credentials that a first credential store is to be accessed to validate the authentication request from the first computer, the first credential store storing sets of credentials that have the same format;

validating the first set of credentials provided by the user by accessing the first credential store to determine whether the first set of credentials is associated with a single unique user identifier, wherein ~~the first~~each set of credentials in the first credential store ~~are~~is associated with a single unique user identifier of ~~the~~ a user, a single unique user account, and a single unique user profile such that upon determining that the first set of credentials is associated with a unique user identifier, the unique user identifier is returned to the first computer such that the desktop computer may use the unique user identifier to access a service;

receiving a second authentication request at the authentication system from a second computer, wherein the authentication request includes a second set of credentials of the user, the second set of credentials ~~being~~ having a format that is different than the format of the first set of credentials;

determining based on the format of the second set of credentials that a second credential store is to be accessed to validate the authentication request from the second computer, the second credential store storing sets of credentials that each have the same format; and

validating the second set of credentials provided by the user by accessing the second credential store to determine whether the second set of credentials is associated with a single unique user identifier, wherein ~~the second~~each set of credentials in the second credential store ~~are~~is also associated with ~~the~~ a single unique user identifier of ~~the~~ a user, ~~the~~ a single unique user account, and ~~the~~ a single unique user profile such that upon determining that the second set of credentials is associated with the same unique

user identifier as the first set of credentials, the unique user identifier is returned to the second computer such that the second computer may use the unique user identifier to access the service.~~, such that the user may access the single unique user account by entering either the first set or the second set of credentials.~~

49. (Previously Presented) The method of claim 48, wherein the first and second computer are the same computer, and wherein the first set and second set of credentials comprise a username and password, and wherein the username of the first set of credentials is different than the username of the second set of credentials.

50. (Previously Presented) The method of claim 49, wherein the username of first set of credentials is an email address having a first domain and the username of the second set of credentials is an email address having a second domain that is different than the first domain.